AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The Apple ID "RUFFYMANJOE@GMAIL.COM" Account, controlled by Apple Inc., headquartered at One Apple Park Way, Cupertino, California as further described in Attachment A.

Case No. MJ21-5153

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
The Apple ID "RUFFYMANJOE@GMAIL.COM" Account, controlled by Apple Inc., headquartered at One Apple Park Way, Cupertino, California, as further described in Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B for a list of infromation to be disclosed, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. §§ 1343, 1349, 1028A, 1956, and 1957	Wire Fraud, Conspiracy, Aggravated Identity Theft, and Money Laundering

The application is based on these facts:

See attached Affidavit of FBI Special Agent Andrea DeSanto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea L. DeSanto
Applicant's signature

FBI Special Agent Andrea L. DeSanto
Printed name and title

The above-named agent provided a sworn statement attesting to the truth of the attached affidavit by telephone.

Date: July 8, 2021

Judge's signature

City and state: Tacoma, Washington

J. Richard Creatura, United States Chief Magistrate Judge
Printed name and title

AFFIDAVIT OF SPECIAL AGENT ANDREA L. DESANTO

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, ANDREA L. DESANTO, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. ***Purpose of the Affidavit:*** I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since 2006. I am investigating a massive fraud on the Washington Employment Security Department ("ESD"), in which criminals submitted hundreds of millions of dollars of fraudulent Pandemic Unemployment Assistance claims and other CARES Act benefits using the stolen personal identifying information of thousands of Washington residents. This conduct violated numerous federal criminal statutes, including Title 18, United States Code, Sections 1343 (wire fraud), 1956 and 1957 (money laundering), 641 (theft of public funds), 371 (conspiracy), and 1028A (aggravated identity theft).

2. In furtherance of this investigation, I am seeking a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with Apple ID "RUFFYMANJOE@GMAIL.COM" (the "TARGET ACCOUNT") that are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California, 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

3. As discussed herein, my investigation has developed evidence that the TARGET ACCOUNT is controlled by an individual who personally submitted claims seeking in excess of $350,000 of COVID-19 related unemployment benefits and has engaged in a history of submitting fraudulent disaster claims to other federal agencies and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

fraudulent tax returns to the Internal Revenue Service ("IRS"). Based on my training and experience and the facts as set forth in this affidavit, I have probable cause to believe that the TARGET ACCOUNT will contain evidence of the unemployment fraud and may enable investigators to identify co-conspirators and other COVID-19-related benefits or loan fraud. Accordingly, I submit that there is probable cause to believe that the information described in Attachment A contains evidence of violations of Title 18 United States Code, Sections 1343 (wire fraud), 1349 (conspiracy), 1028A (aggravated identity theft), and 1956 and 1957 (money laundering) as described in Attachment B.

4. The information set forth in this affidavit is not intended to detail each and every fact and circumstance of the investigation or all information known to me or the investigative participants. Rather, this affidavit is intended to present the facts relevant to the issue of whether there is probable cause to issue the requested search warrant.

5. ***Agent Background and Experience:*** I am currently assigned to the Seattle Field Office. My primary duties include investigating violations of federal law, including but not limited to, Title 18, United States Code, Sections 1343 (wire fraud), 1028A (aggravated identity Theft), 1956 (money laundering), 1957 (transactional money laundering), and conspiracy to commit these offenses. I previously worked on the Cyber squad, where I primarily investigated computer intrusions and other cybercrimes. My experience as an FBI agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. In addition to my experience with cybercrime investigations, I also have experience with financial investigations. I have received formal training on tracing the financial proceeds of crimes. I have applied that training in the context of numerous investigations in which I have reviewed records from financial institutions both in the United States and in foreign jurisdictions, in order to identify the proceeds of criminal offenses under investigation.

6. Based on my training and experience, I am familiar with the ways in which individuals involved in fraud schemes use shell e-mail accounts, computers, cellular telephones, Internet Protocol ("IP") addresses, bank accounts, synthetic identities, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

counterfeit documents to facilitate fraudulent activity. I have learned that individuals perpetrating computer intrusions and identity theft-related bank fraud and wire fraud schemes employ a number of techniques, either alone or in combination, to further their illegal activities and to avoid detection by law enforcement. These techniques include: utilizing web-based email accounts and other electronic messaging accounts to send, receive, store, and obtain personal identifying information, such as dates of birth and bank and credit card account numbers and related information; and the use of cloud-based accounts to communicate and store information and tools related to the fraud. I know that individuals involved in fraud schemes often establish shell e-mail accounts and e-mail addresses in fictitious names and/or in the names of third parties in an effort to conceal their identities and illicit activities from law enforcement. I know that individuals involved in fraud often use virtual private network ("VPN") accounts and Internet hosting services to conceal their true identities and geographical locations from law enforcement or other entities.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATEMENT OF PROBABLE CAUSE

A. Background

8. Based on publicly available information, I know that on March 27, 2020, the United States enacted into law the Coronavirus Aid, Relief, and Economic Security ("CARES") Act. The CARES Act authorized approximately $2 trillion in aid to American workers, families, and businesses to mitigate the economic consequences of the COVID-19 pandemic. The CARES Act funded and authorized each state to administer multiple new unemployment benefits, including additional weekly payments

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and extension of benefits after regular benefits are exhausted ("CARES Act unemployment benefits"). The CARES Act allows an unemployed worker to obtain back benefits retroactive to the date on which the applicant was affected by COVID 19, which, under program rules, may be as early as February 2, 2020.

9. CARES Act unemployment benefits are funded by the United States government through the Department of Labor and administered at the state level by state agencies known as state workforce agencies ("SWAs"). The Washington Employment Security Department ("ESD"), the State of Washington agency responsible for administering unemployment benefits, is the SWA for the State of Washington. Applicants apply for ESD-administered benefits using Washington's SecureAccess Washington (SAW) web portal and an ESD-administered site known as the Unemployment Tax and Benefit (UTAB) system.

10. I know from my contact with other law enforcement officers that, beginning on around April 20, 2020, officials began receiving complaints from employers about potentially fraudulent unemployment claims. The employers reported that they had received notices from ESD indicating that persons still under their employ had filed unemployment claims. For example, on or about April 20, 2020, the Seattle Fire Department ("SFD") notified the U.S. Attorney's Office for the Western District of Washington that claims had been filed in the names of multiple firefighters who were actively employed by SFD. SFD reported that it had interviewed the firefighters, who had denied any involvement in the claims. Other employers, including Microsoft Corporation, the City of Bellingham, Zulily, and Seattle Yacht Club submitted similar complaints.

11. Roughly around that same time, numerous other agencies, including the FBI, the Social Security Administration Office of Inspector General, the United States Secret Service, the Department of Labor Office of the Inspector General, the United States Postal Inspection Service, and Internal Revenue Service Criminal Investigation, joined the investigation. Agents from these agencies, including myself, have reviewed

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

voluminous financial records and databases reflecting the fraudulent transactions and have conducted dozens of interviews.

12. The investigation has developed evidence that hundreds of millions of dollars of fraudulent claims were filed with ESD using the stolen personal identifying information of Washington residents. The FBI investigation has determined that many of the fraudulent claims were filed using IP addresses that resolve to Nigeria. While the actual amount of loss is unknown, the Washington State Auditor has issued a report finding that ESD paid out at least $642,954,417 in fraudulent imposter claims, of which $369,789,082 has been recovered.

C. Role of Gmail Accounts in the Fraud

13. ESD provided the government with data identifying the email accounts associated with claims submitted over the period of the fraud. The data indicate that thousands of different email accounts, including accounts operated by Google, were used in connection with the filing of the fraudulent claims. For many of these Google email accounts, perpetrators took advantage of a particular feature of Google email accounts that allowed them to submit multiple fraudulent claims from a single Google email account, without ESD detecting that a single email address was being used repeatedly. Specifically, in routing emails to an email box, Google disregards periods in the email address, meaning that the email address "john.doe@gmail.com" and "johndoe@gmail.com" will resolve to the same Google email account, even though ESD identifies them as two different accounts. Two email addresses like these that are distinguished only by periods are known as "Google variants" or "dot variants." I know from my training and experience that criminals sometimes take advantage of this feature to make it appear that emails are originating from multiple accounts, when in fact they originate from the same account. This reduces the number of email accounts that a criminal must open and monitor while perpetrating a fraud, while avoiding fraud alerts that may be triggered when multiple claims originate from the same account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

D. Use of the sandytangy58@gmail.com Account

14. Investigators analyzed ESD's database to identify Gmail accounts that were used to submit multiple claims using the Google dot variant method discussed above. Among these accounts was an account with the address sandytangy58@gmail.com.

15. According to a Department of Labor Office of Inspector General's Office analysis of ESD's claims database, dot variants of sandytangy58@gmail.com (such as san.dyta.ngy58@gmail.com, sa.ndyt.a.ngy58@gmail.com, and san.d.y.t.an.gy58@gmail.com.) were used to submit approximately 102 claims for ESD benefits exceeding $350,000. The Department of Labor's analysis also indicates the account was used to submit one or more claims to the SWAs for Hawaii, Maine, Michigan, Missouri, Montana, New York, Ohio, Pennsylvania, Wisconsin, and Wyoming.

E. Identification of RUFAI

16. On June 19, 2020, the government applied for, and the Honorable Paula L. McCandlis, entered an order pursuant to 18 U.S.C. § 2703(d) directing Google to produce non-content material associated with the sandytangy58@gmail.com account. Subsequently, on January 29, 2021, the Honorable Michelle L. Peterson issued a search warrant to Google for the sandytangy58@gmail.com account. Google responded to the search warrant on approximately February 5, 2021. The responses to the order and search warrant yielded evidence linking RUFAI to the account and evidence of fraud in the account, as specified below.

17. The § 2703(d) order required Google to identify, *inter alia*, the recovery SMS number for the account. Based on my experience and open source research, I know that Google uses recovery SMS numbers as an alternate means to communicate with the account holder, including for purposes of two-step authentication and password recovery if the account holder forgets his or her password. I know from my training and experience that email account users ordinarily provide their own cell phone number as an SMS recovery number so that they can easily validate their account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

18. Google's response to the § 2703(d) order indicated that the recovery SMS number associated with sandytangy58@gmail.com was the Nigeria-based number 234-909-874-2695 (the "Sandytangy58 SMS Number"). Investigators conducted research into the Sandytangy58 SMS Number. They determined that this number was listed on a visa application of a Nigerian man named ABIDEMI RUFAI that was submitted to the State Department on July 7, 2019.

19. Additionally, international travel records show that RUFAI entered the United States on February 19, 2020, and left the country on August 9, 2020, and was therefore apparently present in the United States during the period of the fraud. I have reviewed financial reporting showing that within that timeframe, between March 3, 2020 and August 2, 2020, a Citibank checking account in RUFAI's name received a total of $288,825 in deposits, and $236,701 was transferred out of the account over the same period.

20. When RUFAI arrived in the United States, he reported to the United States government that he would be staying at his brother's apartment on Guy R. Brewer Boulevard in Jamaica, New York. The investigation has developed evidence that some of the fraud proceeds were sent by FedEx to this address. Specifically, I have reviewed information from a financial institution reporting that on May 19, 2020, a Richland, Missouri resident with the initials C.S. received an ACH transfer of unemployment benefits from ESD in the amount of $9,920. ESD records indicated that this payment was based on a claim submitted to ESD on May 18, 2020, in the name of a Washington resident with the initials M.S. using the email address s.a.n.dy.t.an.gy58@gmail.com. Also on May 19, 2020, C.S.'s account received two ACH transfers totaling $8,650 from the Maine Department of Labor. When questioned by her credit union about the transfers, C.S. stated that she had withdrawn $11,000 of the funds and sent them to an address on Guy R. Brewer Boulevard in Jamaica, New York. The address C.S. provided is RUFAI's brother's apartment. On May 10, 2021, M.S. told investigators he had neither filed an unemployment claim or given anyone permission to do so on his behalf.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

21. On May 19, 2021, FBI Special Agent Heidi Hawkins and I interviewed four additional Washington residents with the initials S.C., S.S., N.J., and L.B. ESD received claims with these individuals' names, Social Security numbers, and dates of birth that listed a sandytangy58@gmail.com dot variant as the claim's associated email address. During the course of these interviews, each individual confirmed his or her Social Security number and date of birth. All interviewees also confirmed that they used neither the sandytangy58@gmail.com dot variant email address nor the bank account listed on the claim associated with their identities.

F. Contents of the Email Account and Google Drive

22. The contents of the sandytangy58@gmail.com account included over 1,000 emails from ESD, including the automated activation emails that the SAW system sends when new user sets up an account. The account also contained approximately 100 emails from the SWAs for Hawaii, Wyoming, Massachusetts, Montana, New York, and Pennsylvania. An email attachment with the file name "FRESH WASHINGTON.txt" lists the full name, Social Security number, date of birth, and address of nearly 100 Washington residents, each listed with a dot variant of sandytangy58@gmail.com. Many of the entries also included bank account and credit card numbers and employer names. I have matched approximately 60 of these identities with claims filed with ESD using dot variants of sandytangy58@gmail.com. The account also contained numerous emails from Green Dot, which is a payment system that I know was used to collect and transfer a large share of the claims that were filed with ESD using the sandytangy58@gmail.com account. In addition, the sandytangy58@gmail.com account contained numerous emails from other online payment and cryptocurrency services.

23. In addition, the sandytangy58@gmail.com account contained substantial evidence that the user was actively engaged in stealing and retaining the personal identifying information of American citizens. The account contained large volumes of emails and file attachments with thousands of bank and credit card numbers, personal identifying information such as dates of birth and U.S. addresses associated with first and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

last names, and images of what appear to be driver licenses from various states, including New York. The account also contained a very large volume of tax returns of United States taxpayers. In many of the emails, the user appears to pose as an accountant, signing the email "Sandy Tang CPA."

24. The sandytangy58@gmail.com account also contained emails indicating that the user had submitted other types of fraudulent claims to the United States government. For example, the account contained numerous emails from the Federal Emergency Management Agency (FEMA) from September 2017, which appears to indicate that the user had filed multiple claims for disaster relief during this period. The account also contained emails from an online tax filing service indicating that the user had filed tax returns in the United States. The sandytangy48@gmail.com address was blind carbon copied on what appears to be every email sent to multiple seemingly authentic email addresses, suggesting the user compromised these email accounts using malware or other cyber intrusion method.

25. The search warrant return also contained further evidence RUFAI is the user of the account. The Google search warrant required Google to provide contents of the Google Drive associated with sandytangy58@gmail.com. Google Drive allows users to store documents, files, and other content online so that they can be remotely accessed from anywhere. The Google Drive documents associated with the sandytangy58@gmail.com account included four images of an individual who matches the physical appearance of RUFAI in his 2019 visa application photo and secondary inspection photos taken by U.S. Customs and Border Patrol on and January 19, 2017, and February 18, 2020. In addition, as discussed below, I arrested RUFAI on May 14, 2021, and know from my observations that the photos depict RUFAI. The images had file names with the prefix "Media WhatsApp Images," which indicates that the image at one time was transmitted using WhatsApp, a messaging and voice-over-IP application that allows users to send text and voice messages, make voice and video calls, and share images, documents, and other content. In addition, the contact list for the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

sandytangy58@gmail.com account included the email address bidemi.rufai@yahoo.co.uk, a variation of the email address listed on RUFAI's visa application (bidemi_rufai@yahoo.co.uk).

26. As discussed above, RUFAI submitted a United States visa application on July 7, 2019. Google's response to the search warrant shows that the user of the sandytangy58@gmail.com account conducted an internet search using the term "apply for US visa" on the same day, July 7, 2019. The sandytangy58@gmail.com account also included three confirmation emails from online purchases that list RUFAI's brother's address on Guy R. Brewer Boulevard in Jamaica, New York, as the billing address. For example, the account contains a January 26, 2017 email string in which the user of the sandytangy58@gmail.com account purchased a license to use Sigma Tax Pro software. The billing information on the invoice is "Thuy Le, Sandy S Tang CPA," and lists RUFAI's brother's address on Guy R. Brewer Boulevard as the billing address. Similarly, the sandytangy58@gmail.com account was used to purchase a Verizon wireless refill on February 14, 2017. The billing address for the order is "James Andrus" at the Guy R. Brewer address. Of note, U.S. Customs and Border Patrol records show that RUFAI arrived in New York on January 19, 2017 and remained in this country until May 4, 2017, and therefore was in the country for the period of these transactions.

G. Amended Complaint, Arrest, and Indictment

27. On May 14, 2021, this Court authorized an Amended Complaint charging RUFAI with five counts of wire fraud and issued an arrest warrant for his arrest. That evening, other federal law enforcement agents and I arrested RUFAI after he arrived at John F. Kennedy International Airport, in Queens, New York.

28. Following recorded *Miranda* warnings, RUFAI agreed to speak with FBI Special Agent Heidi Hawkins and me. During that interview, RUFAI confirmed that the Nigeria-based Sandytangy58 SMS Number and U.S.-based 917-992-8410 are his phone numbers. However, he denied any connection to the sandytangy58@gmail.com account or any involvement in submitting fraudulent claims. I showed him two of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

photographs of him that were found on the Google Drive associated with sandytangy58@gmail.com, and he acknowledged that these were photos of him. RUFAI stated that one photo had been stored on his phone and was not publicly available (the other one is posted to Facebook).

29. On May 26, 2021, the Grand Jury indicted RUFAI for one count of conspiracy to commit wire fraud, nine counts of wire fraud, and five counts of aggravated identity theft.

H. The Target Apple Account

30. Among the items seized incident to the May 14, 2021 arrest was a black Apple iPhone 11 wireless phone that RUFAI had in his possession. On May 24, 2021, the Honorable Roanne L. Mann, U.S. Magistrate Judge for the Eastern District of New York issued a search warrant for the Apple iPhone 11 and other items seized incident to arrest ("EDNY Warrant"). The warrant authorized the forensic examination of the Apple iPhone 11 for the purpose for the purpose of identifying electronically stored information ("ESI") relating to violations of Title 18 United States Code, Sections 1343 (wire fraud), 1349 (conspiracy), and 1028A (aggravated identity theft).

31. On June 2, 2021, FBI agents executed the EDNY Warrant and conducted a forensic examination of the Apple iPhone 11. Only a portion of the ESI stored on the Apple iPhone 11 was extractable because the device was locked with an unknown passcode; however, the forensic examination revealed that the phone had been backed up to the iCloud for TARGET ACCOUNT on May 14, 2021. The forensic exam also showed that the latest number used for the iPhone was 917-992-8410, which is the number RUFAI provided as his to Special Agent Hawkins and me on May 14, 2021. The forensic exam further showed that the same iPhone was also previously used for the Nigeria-based Sandytangy58 SMS Number.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

BACKGROUND CONCERNING APPLE[1]

32. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

33. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). Following are some of the services Apple provides that are relevant here:

a. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device.

b. iCloud Backup allows users to create a backup of their device data.

c. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers.

d. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices.

e. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

f. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

h. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

i. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

34. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

35. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

36. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

37. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

38. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

39. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

40. In addition, the user's account activity, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

41. In this case, there is probable cause to believe that the user of the TARGET ACCOUNT belongs to RUFAI. The contents of the Apple account and associated material may provide additional attribution evidence linking the sandytangy58@gmail.com account to RUFAI, including photos that match those found in the sandytangy58@gmail.com Google Drive or internet searches that match those done by the sandytangy58@gmail.com account. The partial extraction from the forensic exam of RUFAI's iPhone shows that a Gmail email application was installed, and the iCloud information may provide additional evidence that RUFAI accessed the sandytangy58@gmail.com account from his iPhone and may have saved documents to his iCloud account.

42. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. The partial extraction from the forensic exam of RUFAI's iPhone included images of banking and financial documents after April 2020 (when the first charged wire fraud conduct occurred) and may involve fraud proceeds from the crimes. Additionally, the forensic exam showed that RUFAI's phone had various banking and finance applications installed, including at least three U.S.-based banks and an application used to purchase Bitcoin. Finally, some of the data extracted from RUFAI's iPhone shows that he used at least one messaging application to receive banking account numbers from multiple individuals. The TARGET ACCOUNT may provide additional evidence identifying RUFAI's co-conspirators and financial institutions used to facilitate the crimes.

43. The partial extraction from RUFAI's iPhone also included images of seaway bills involving the transport of luxury automobiles from New York in July and August of 2020. Based on my training and experience, individuals participating in laundering illicit proceeds often attempt to obfuscate funds through the purchase and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

subsequent sale of luxury automobiles, particularly when transferring the funds from the United States to another country.

44. Based on my training and experience, individuals participating in fraud and identity theft schemes often save documents containing stolen personal identifying information, financial records, or identification documents in cloud storage and computing platforms such as iCloud. In fact, RUFAI used cloud storage and computing service Google Drive to store, *inter alia*, thousands of files containing stolen personal identifying information, tax returns of American citizens, and other documents used to perpetrate fraud. Moreover, during a recorded call on May 27, 2021, while RUFAI was detained at the Metropolitan Detention Center in the Eastern District of New York, RUFAI discusses using his wireless phone to transfer funds out of his own bank account to an associate who has been linked to the target in a separate ESD fraud investigation. Based on information contained in another recorded call on the same day, this associate uses WhatsApp, a messaging and internet voice service, to communicate.

45. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

46. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

47. Based on the foregoing, I believe there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

States Code, Sections 1343 (wire fraud), 1956 (money laundering), 641 (theft of public funds), 371 (conspiracy), and 1028A (aggravated identity theft) will be found in the TARGET ACCOUNT. I therefore request that the Court issue warrants authorizing a search of the TARGET ACCOUNT, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Andrea L. DeSanto
ANDREA L. DESANTO
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit by telephone on the 8th day of July, 2021.

THE HONORABLE J. RICHARD CREATURA
United States Chief Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property to Be Searched

This warrant applies to the electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the Apple account with the Apple ID "RUFFYMANJOE@GMAIL.COM" (the "TARGET ACCOUNT") as well as all other subscriber and log records associated with the TARGET ACCOUNT, which are located at premises owned, maintained, controlled or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Things to be Seized

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 2, 2021, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

I. Material to be Produced by Apple

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from January 13, 2017 to the present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. The contents of all instant messages associated with the account for the period January 13, 2017 to the present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Material to be seized by the government

Upon receipt of the information described in Section I, the government may seize the following material that constitutes evidence and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1349 (conspiracy), 1028A (aggravated identity theft), and 1956 and 1957 (money laundering) for the TARGET ACCOUNT:

a. Records and information referring or relating to unemployment benefits or any other COVID-19 related government assistance;

b. Records and information relating to the laundering of criminal proceeds, the creation and maintenance of financial accounts, financial transfers and transactions, the possession of monetary instruments, and the disbursement of funds;

c. Records and information relating to stolen personally identifiable information;

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner;

e. Records and information that serves to identify any person who uses or accesses or who exercises in any way any dominion or control over the TARGET ACCOUNT;

f. Records and information that may reveal the current or past location of the account users;

g. Records and information that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;

h. Records and information relating to the subscriber's state of mind as it relates to the crimes under investigation.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970